IoT Security Platform

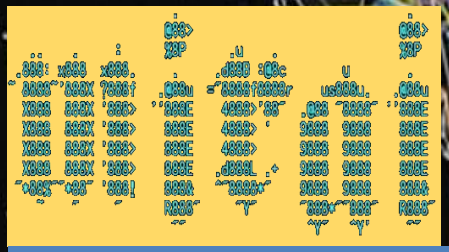
Andrey Doukhvalov
Head of Future Tech

Industrial Cybersecurity: Safegarding Progress
Saint Petersburg, Russia
September, 2017

IoT Malware in Action

- In 2016 one million devices have been infected with **BASHLITE**.
- 96 % are IoT devices (cameras and DVRs),
- 4% are home routers
- 1% are compromised Linux servers.

- **Remaiten** is a Malware which infects Linux on embedded systems by brute forcing using frequentl y used default username and passwords combinations from a list in order to infect a system

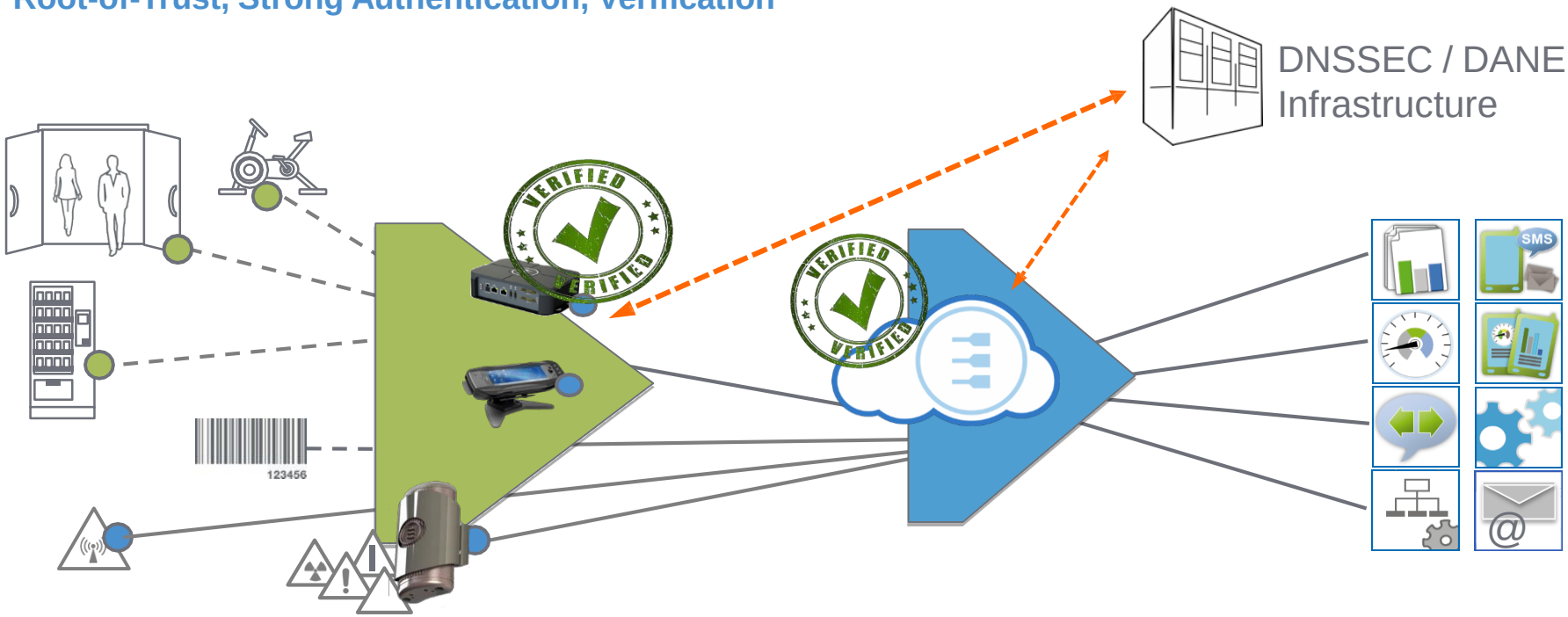


- **Linux.Darlloz** is worm which infects Linux em bedded systems. It targets the internet of things a nd infects routers, security cameras, set-top boxe s by exploiting a PHP vulnerability

- 900,000 customers of German ISP **Deutsche Telekom**
- 2,400 home routers across the UK

IoT Security Landscape

Root-of-Trust, Strong Authentication, Verification



Edge ⟷ **Gateways / Smart Devices** ⟷ **Network** ⟷ **DataCenter/ Cloud**

- Authentication (verified)
- Service discovery / provisioning / pairing
- Trusted execution environment
- Network security / firewall
- Secure Boot

IoT Device Security

- Authentication (verified)
- Encryption
- Message integrity
- MitM protection
- DNS spoofing protection

Communication Security

Authentication (verified)
- PKI / certificate management
- Trusted execution environment
- Network security / firewall
- Access control (role based)

Cloud Security

IoT Developer Survey 2017

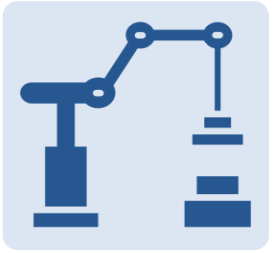
KASPERSKY lab

HOME AUTOMATION

=

IOT PLATFORM

=



INDUSTRIAL AUTOMATION

↗

ENERGY MANAGEMENT

↗

CONNECTED CITIES

↗

- The Eclipse IoT Working Group, IEEE IoT, AGILE IoT and IoT Council co-sponsored an online survey to better understand how developers are building IoT solutions.
- The survey was open from February 7 until March 17, 2017.
  A total of 713 individuals participated in the survey. Each partner promoted the survey to their communities through social media and web sites.

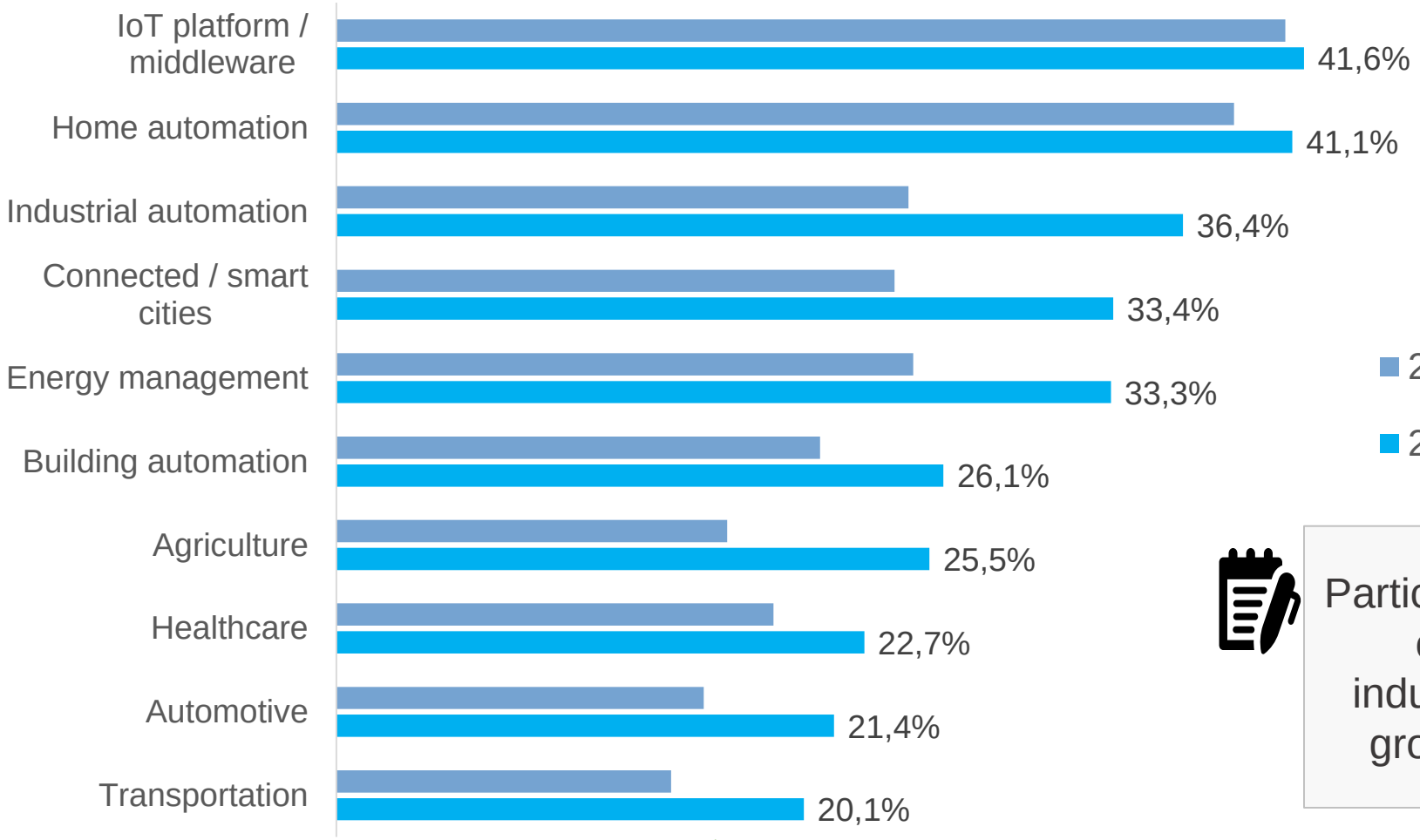
iot eclipse.org

IEEE Internet of Things

AGILE

council

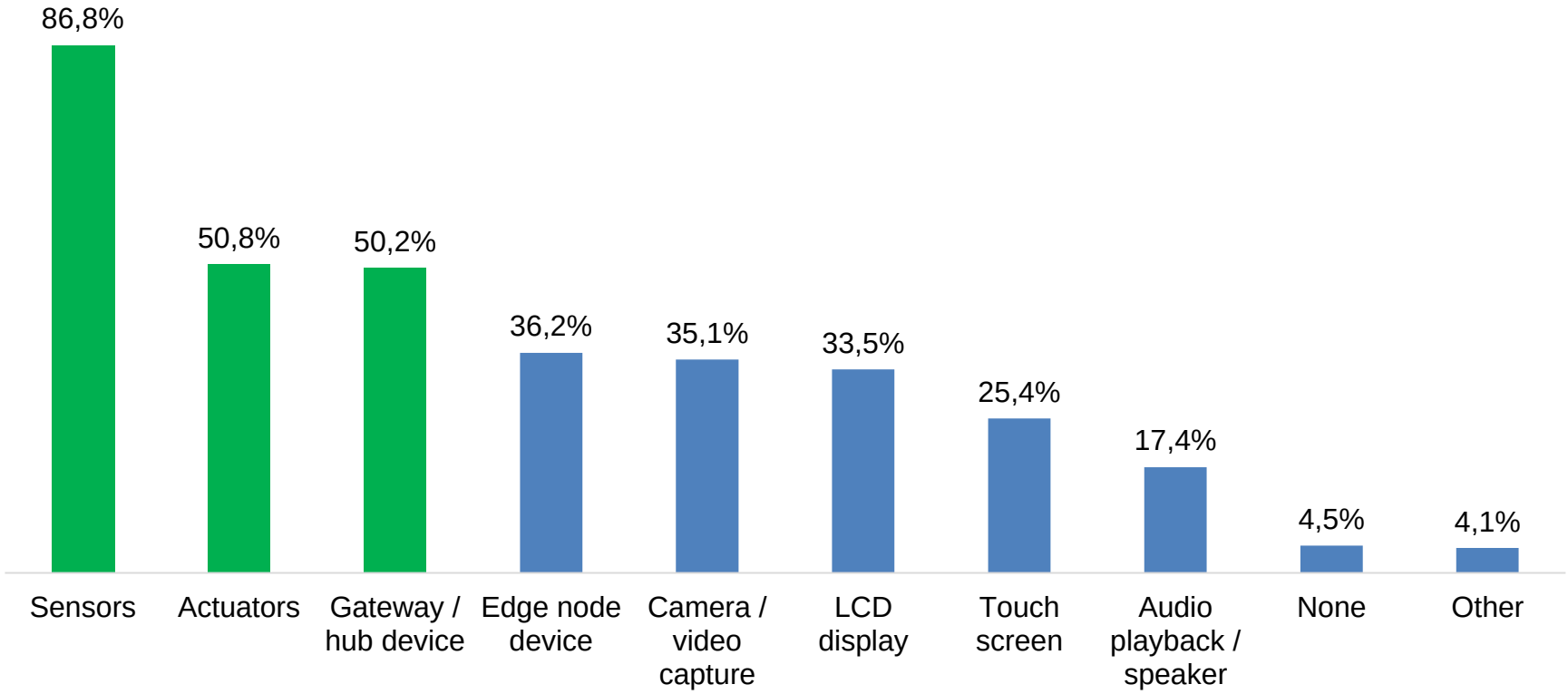
Key Industries / Trends 2016-2017



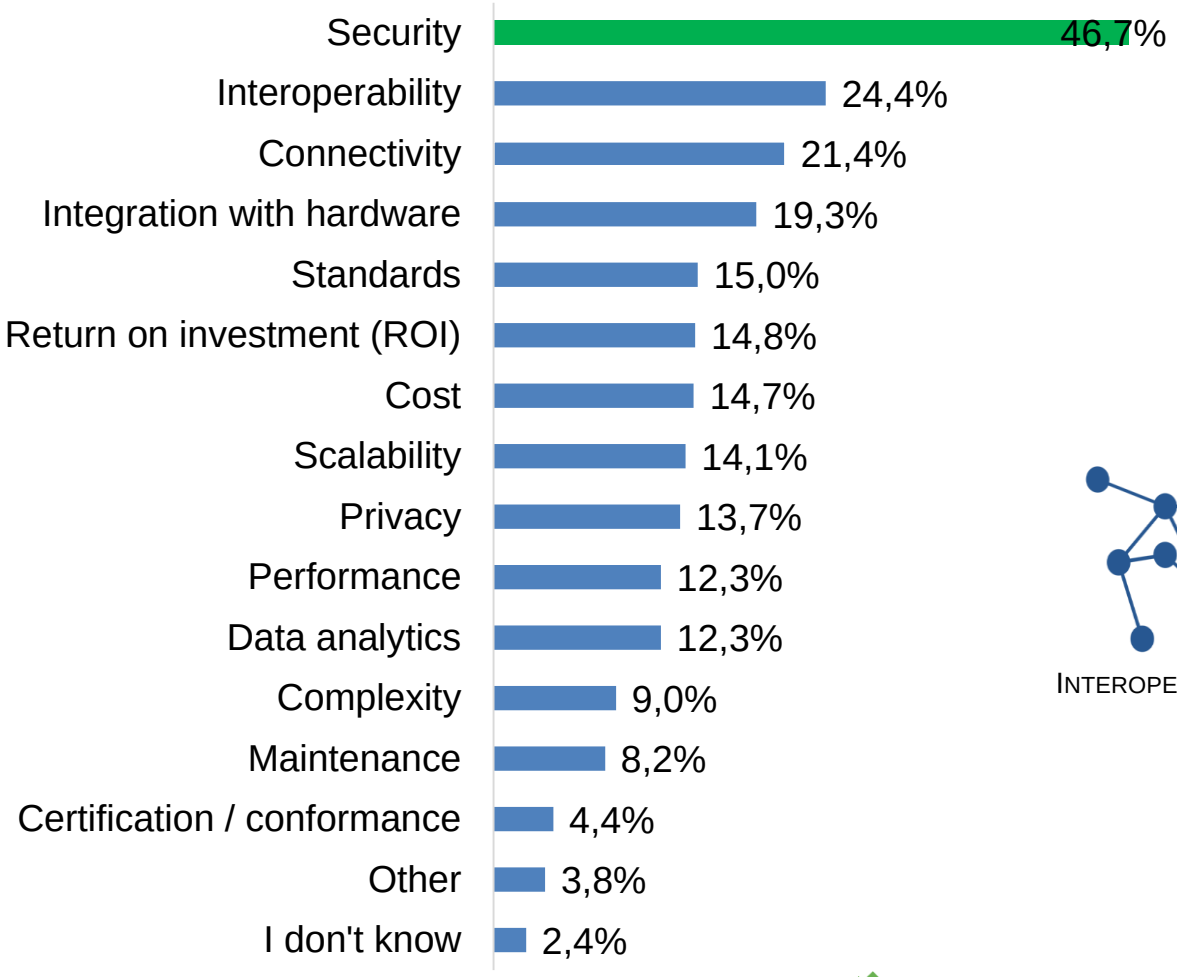
Participation of other industries is growing…

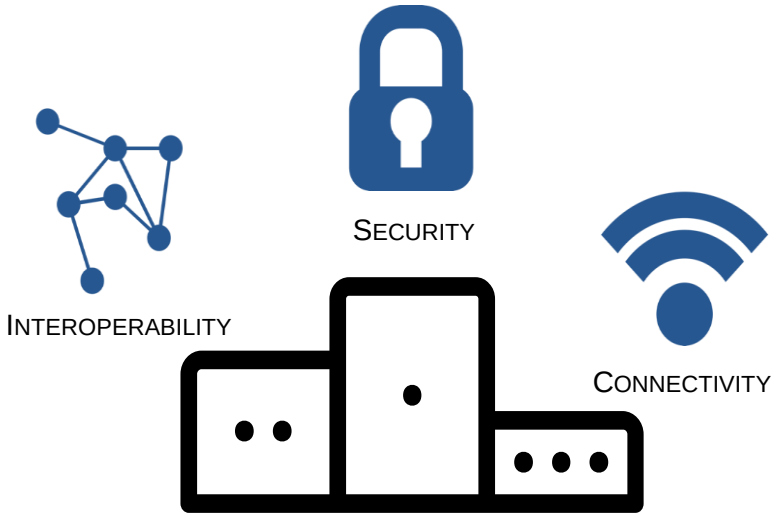
Hardware Components in IoT Solutions

What hardware components are included in your IoT solution?

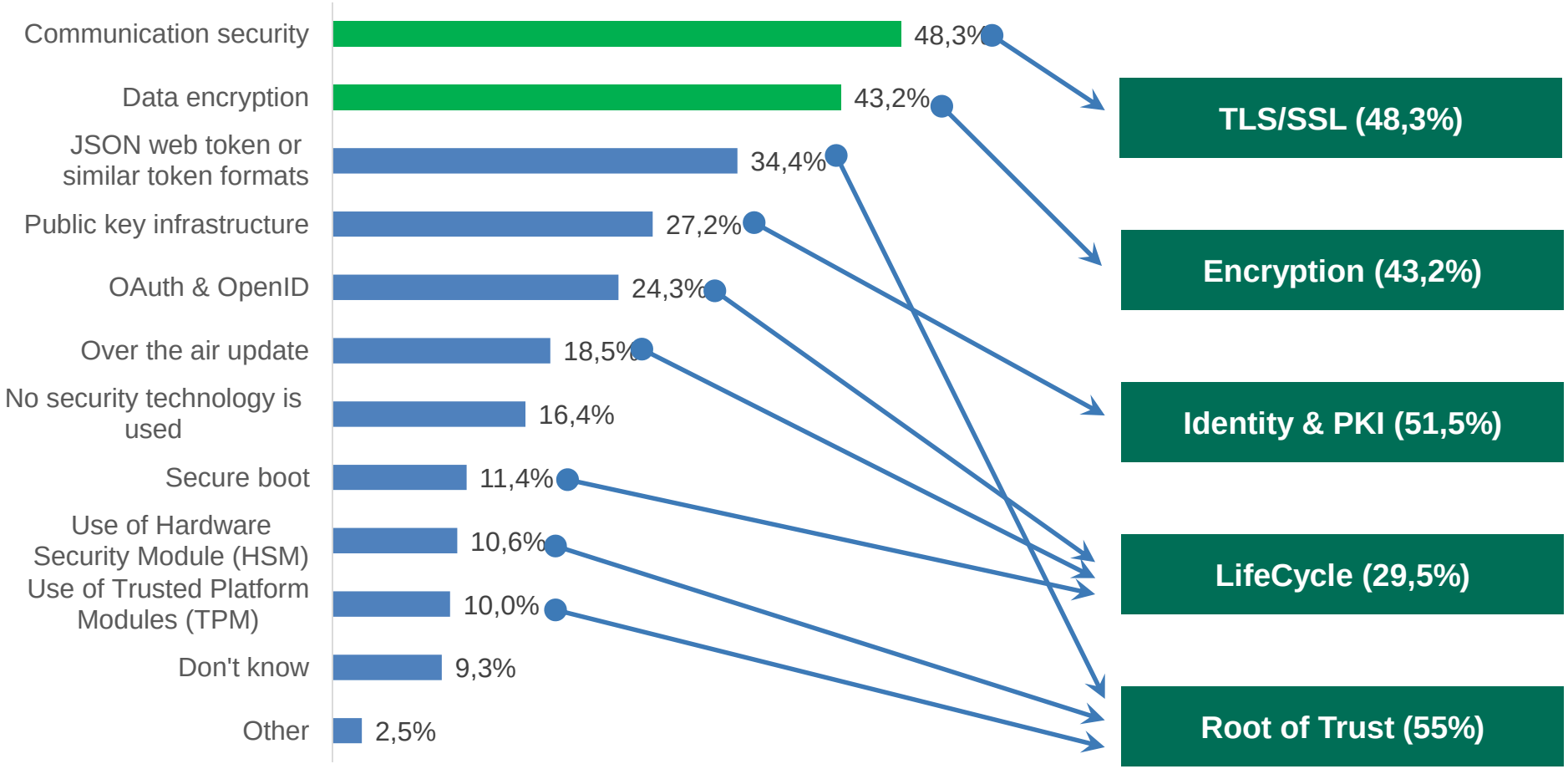


Security is the N1 IoT Developers' concern





IoT Security Technologies

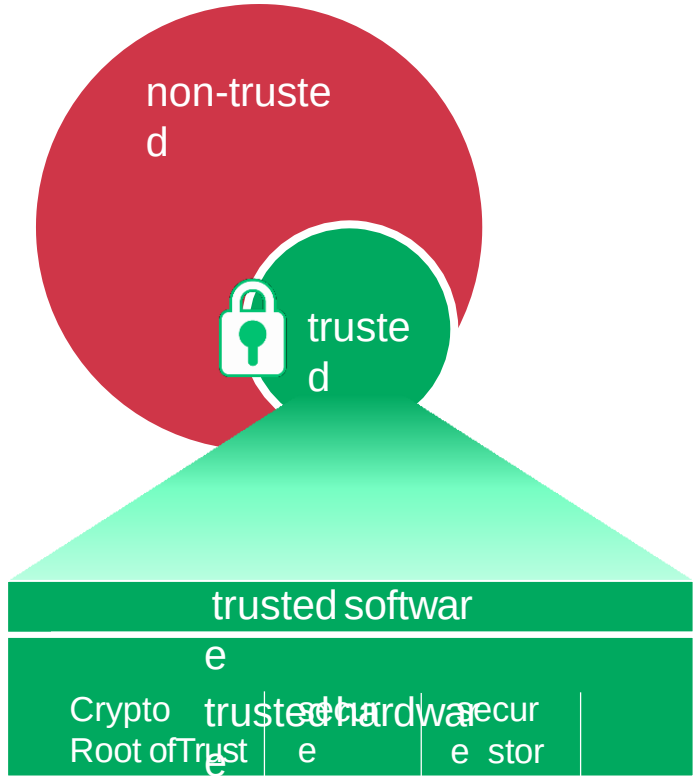


What can we learn from mobile & apply to IoT?

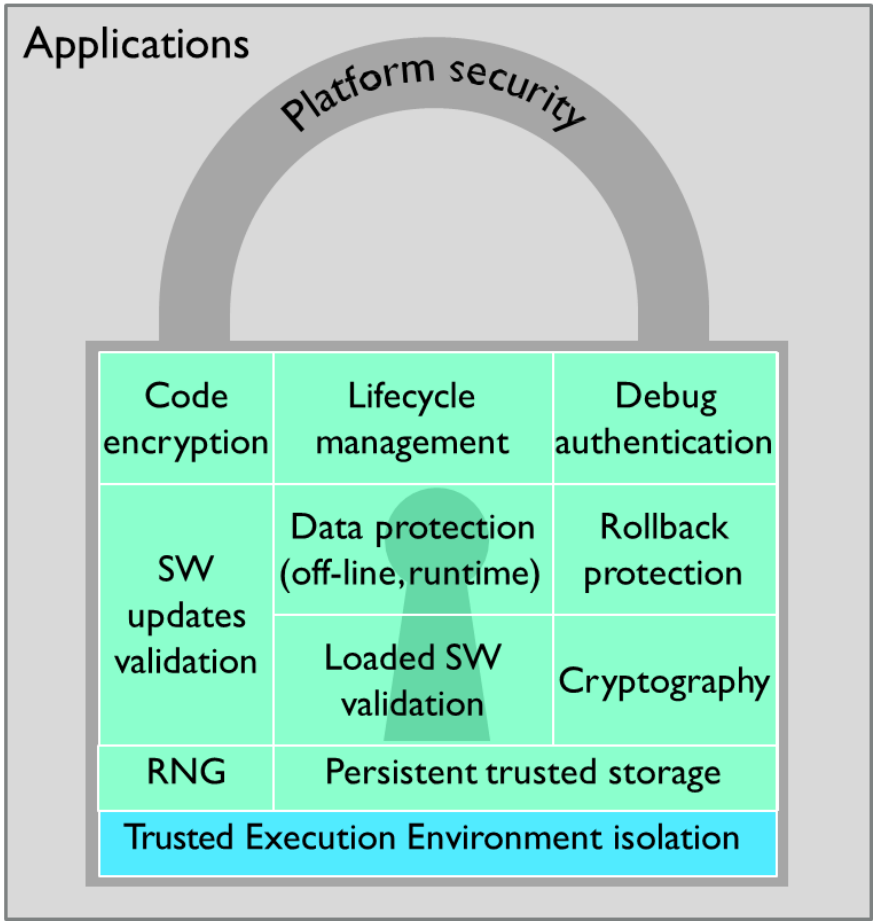
Lifecycle Securi

Communications Secur

Device Securi



IoT Security should be integrated



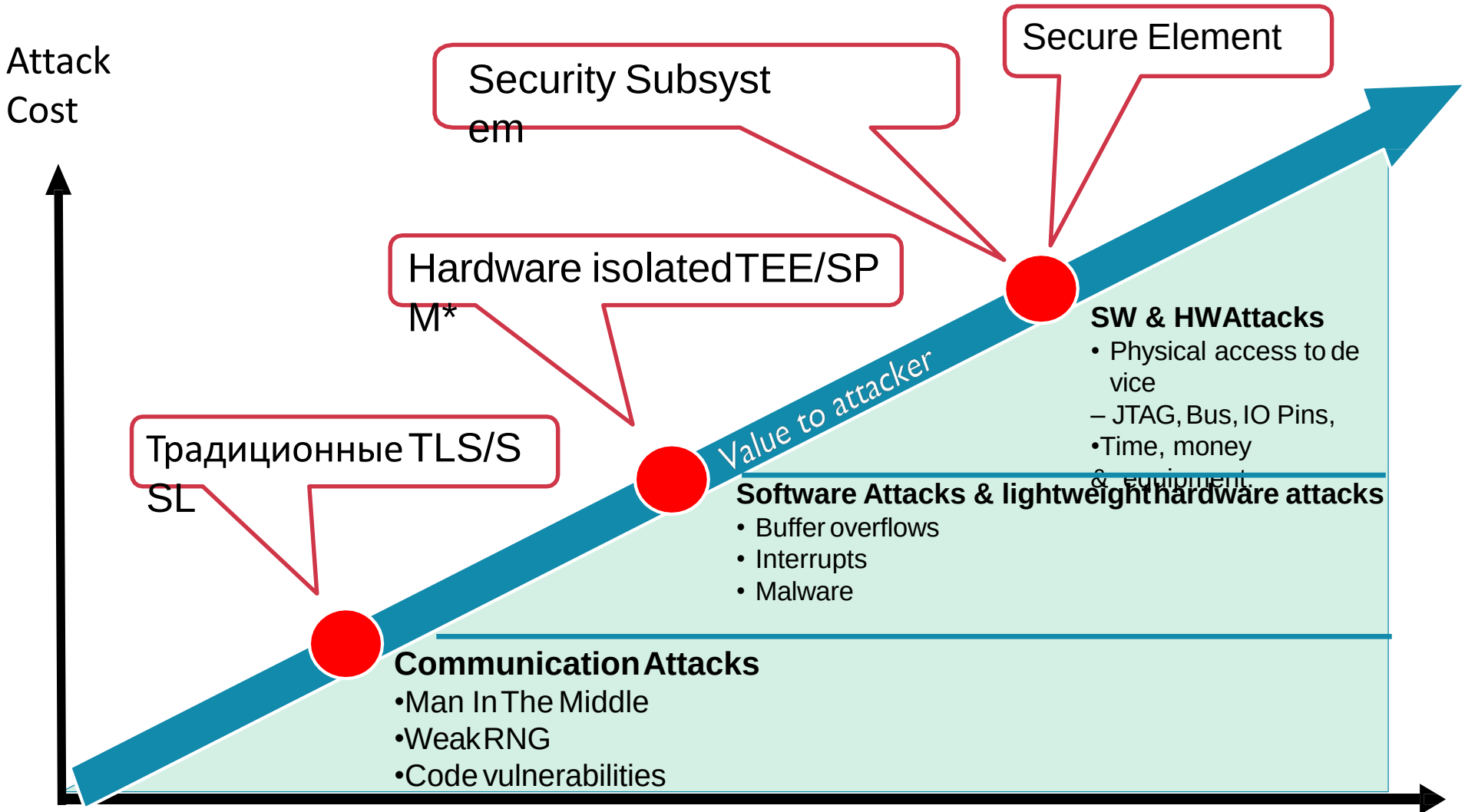
Situation

- Most IoT developers are not security experts
- Little to no knowledge of hardware
- Prior experience in mobile app development
- Time to market & functionality beat security

Strategy

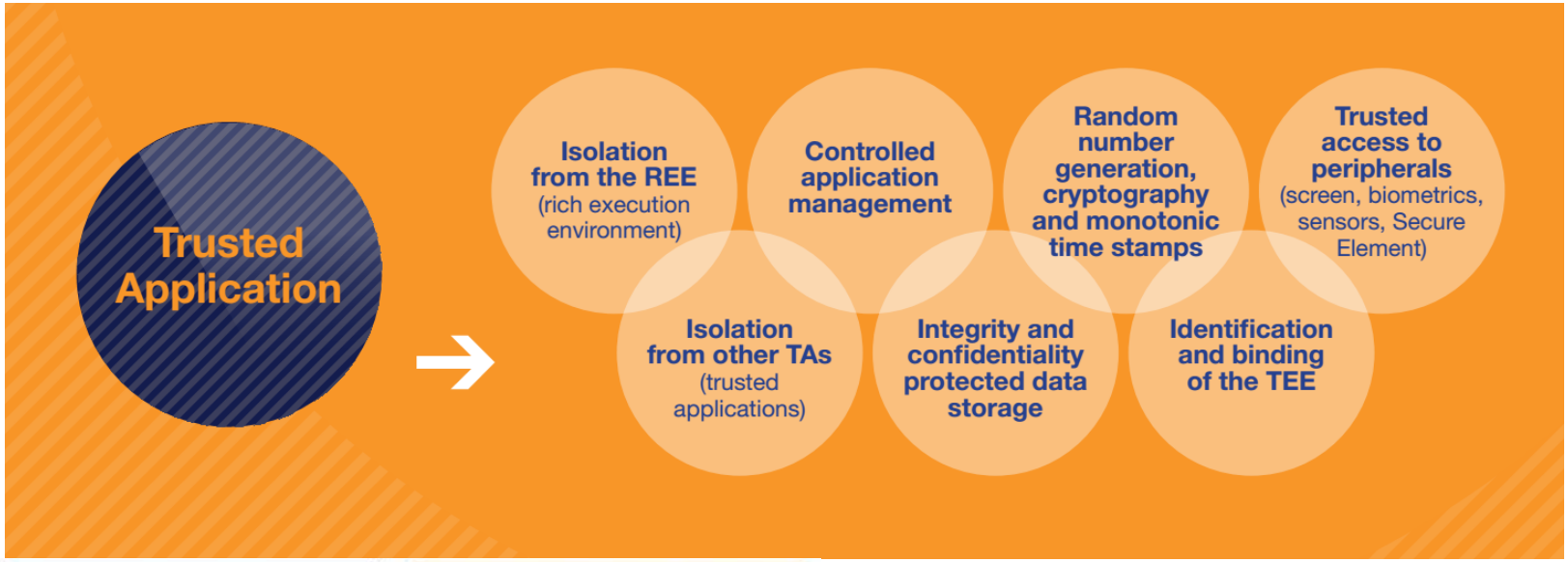
- Ease of use requirements on tools & IoT platform providers
- Hide complexity of hardware based security
- Provide built-in security functions
- Use standard methods and building blocks

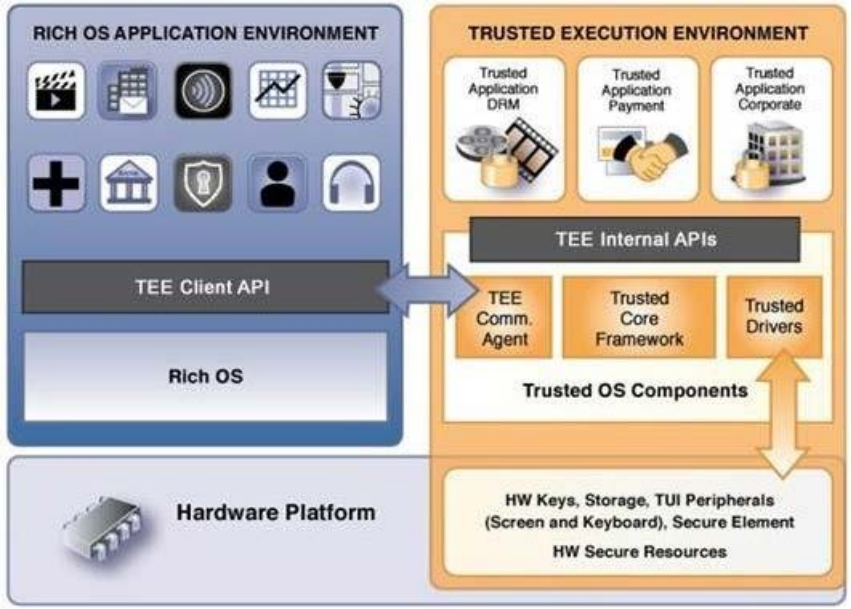
How much security you need ?



*Trusted Execution Environment / Secure Partitioning Man ager

GlobalPlatform Trusted Execution Environment

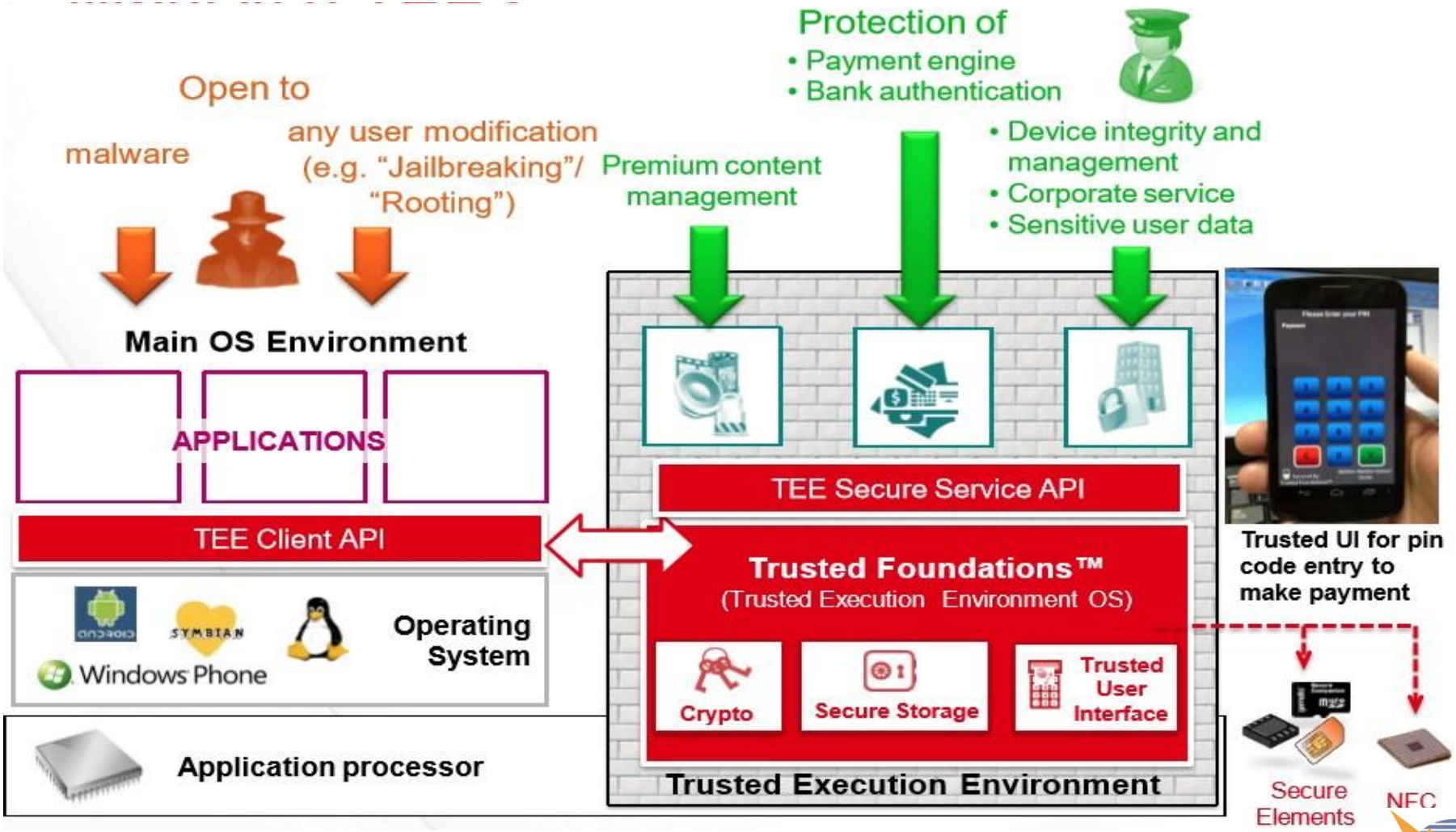




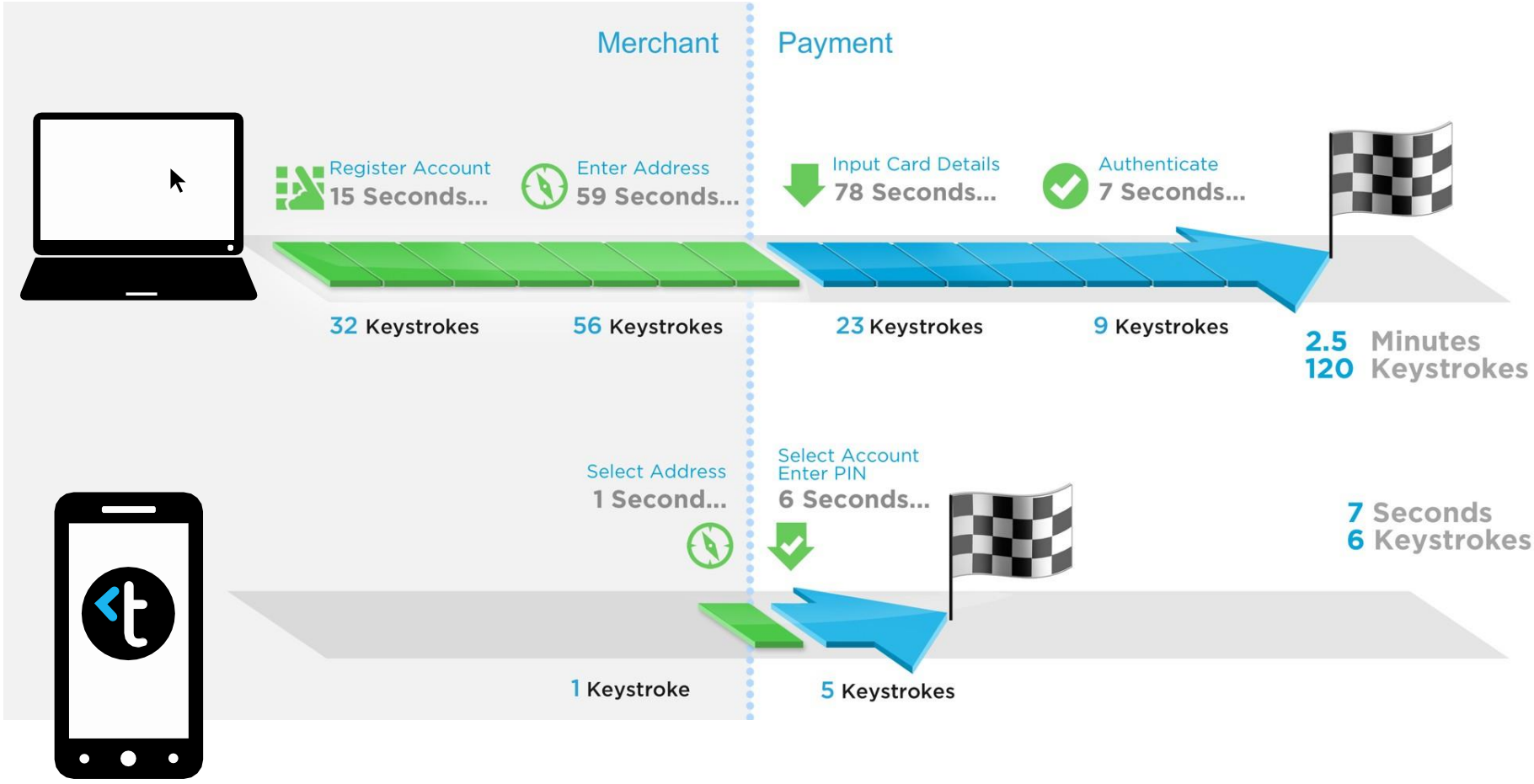
В 2010, под эгидой GlobalPlatform был запущен проект Trusted Execution Environment (TEE). Инициатива была запущена в ответ на изменения на рынке мобильности: требования к безопасности существенно возросли по мере того как потребители начали использовать мобильные устройства для финансовых и платежных транзакций. Кроме того, по мере роста потребления контента (видео, музыка) на разных типах устройств, старые методы защиты контента оказались недостаточны. Для защиты премиального контента его владельцы традиционно использовали Digital Rights Management (DRM), Conditional Access (CA) и др. подобные схемы часто использовали аппаратно-усиленную защиту контента, в то время как теперь они столкнулись со средой где взаимодействует множество разных агентов.Кроме того, изменение путей доставки контента (3G, 4G, Wi-Fi, WiMAX, Bluetooth, NFC) предъявляет повышенные требования к коммуникационным каналам.

Global Platform Trusted Execution Environment

- *TEE became the global standard for embedded security*

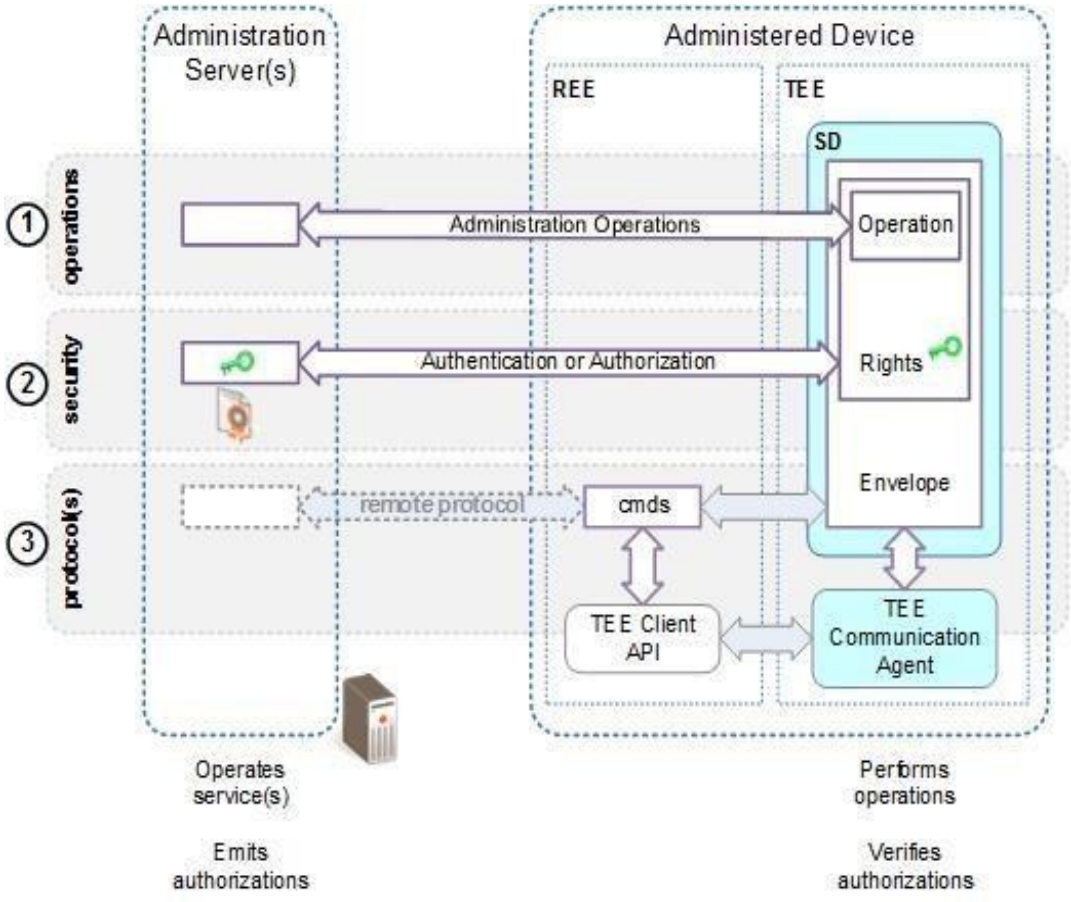


TEE Platform in action



Global Platform TEE Management Framework

- *The newly emerging TEE MF standard lays ground to the remotely controlled embedded security*

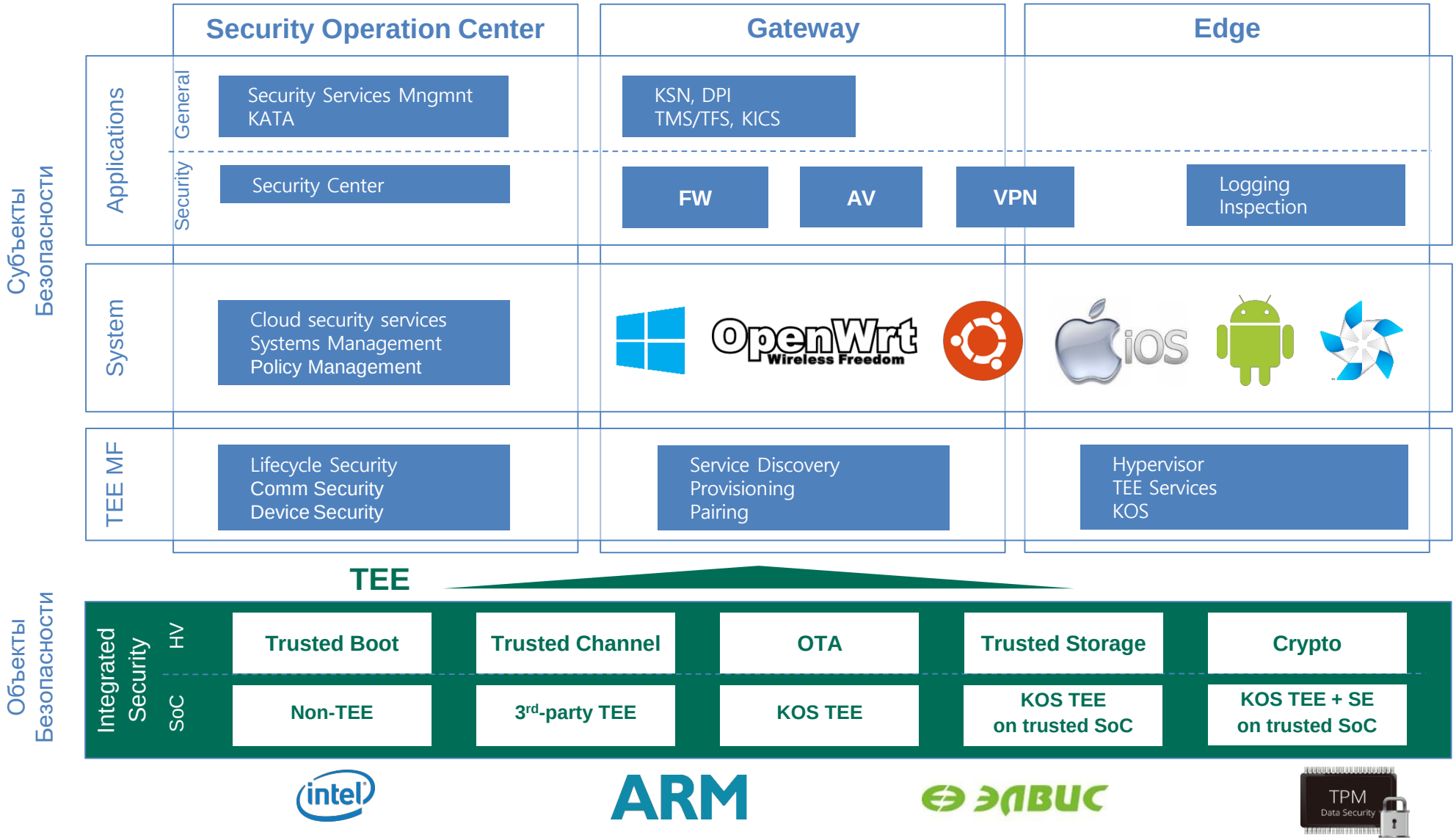


The goals of the security model for administrationare:

- to provide means to manage the Trusted Execut ion Environment (TEE), Security Domains (SD), and Trusted Applications(TA),
- to ensure the security and the integrity of these e ntities,
- to enable the confidentiality of the data,
- to provide a scalable model allowing deployments involving a unique Actor or multiple Actors,
- and to enforce the security policy of each Actor w hile preserving its assets.

To ensure the security and integrity of these entities, th e TMF code implementation on the device is a Trusted OS Component (see [TEE Arch]), or composed from a group of such components. As such it inherits the same security requirements as other Trusted OS Component s.

Kaspersky IoT Security Platform - proposal



Platform Roadmap

	Services	KL Core Assets	Ecosystem
Security Operation Center	Anomaly Detection	MLAD/KATA	Industrial Modules
	Malware Protection	KSN/CF/AV	Security Services
	IoT Platform Connectors	KSC for IoT (TEE MF)	Trusted IoT Platform
Gateway/Networking	Trusted Monitoring	KSN/CV/AV/TMS/KICS	Industrial Protocols
	Lifecycle Security	Firmware Update	Add-Ons
	Communication Security	Trusted Channel	Devices (Router, STB)
	Device Security	Device Pairing	Devices (Router, STB)
Device Level	System Security	KSS (Lib -> Agent)	KSS Linux
	Trusted Hypervisor	KSH	TEE functions
	Integrated Security	KOS	SoC (Elvis)

IoT Security Platform

Lets discuss it

Andrey Doukhvalov
Head of Future Tech

Industrial Cybersecurity: Safegarding Progress
Saint Petersburg, Russia
September, 2017